MACHINE LEARNING-BASED DDOS DEFENCE MECHANISMS IN SOFTWARE-DEFINED INTERNET OF THINGS ENVIRONMENTS

A SYNOPSIS

Submitted by

D. KAVITHA
(Reg. No. 201608248)

in partial fulfillment for award of the degree

of

DOCTOR OF PHILOSOPHY

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING
SCHOOL OF ELECTRONICS AND ELECTRICAL TECHNOLOGY
KALASALINGAM ACADEMY OF RESEARCH AND EDUCATION
(DEEMED TO BE UNIVERSITY)
ANAND NAGAR, KRISHNANKOIL - 626 126
TAMIL NADU, INDIA

SEPTEMBER 2024

1. INTRODUCTION

In recent times, software-defined network architecture has, increasingly, been driving innovative network administration methods and become popular as a result. SDN switches do not handle incoming packets. When an incoming packet arrives, they check their forwarding tables for a match before despatching it to the controller for processing. The controller is the operating system of SDNs. A network of controllers, each connected to a system of switches, constitutes SDN architecture.

DDoS attacks on SDNs have surfaced as a major issue in recent years and their mitigation has gained traction with numerous studies proposing solutions. Figure 1 depicts the ongoing research employing SDN testbeds on SDN security on the control and data planes as well as communication across the two planes. This research explores network security in SDNs, built on a combination of existing methods, and proposes a DDoS attack detection framework in a distributed multicontroller-based SDN environment.

The attacks can be categorized in terms of applications, hosts, resources, networks, and infrastructure. SDNs have made network management easy with all kinds of end devices, including the IoT devices used by 90% of all organizations today. IoT devices, which are indispensable to real-life applications, are invaluable in detecting natural calamities [1]. Given that IoT-enabled devices are spread across swathes of public and private locations, they are easily susceptible to attacks, specifically Distributed Denial-of-Service (DDoS) attacks [2].

SDNs work better with IoT devices than with traditional IP networks, facilitating the free flow of forwarding and routing information to SDN-based switches with little controller intervention [3]. DDoS attacks originate from IoT endpoints at the infrastructure layer and target resources using an SDN-controlled testbed.

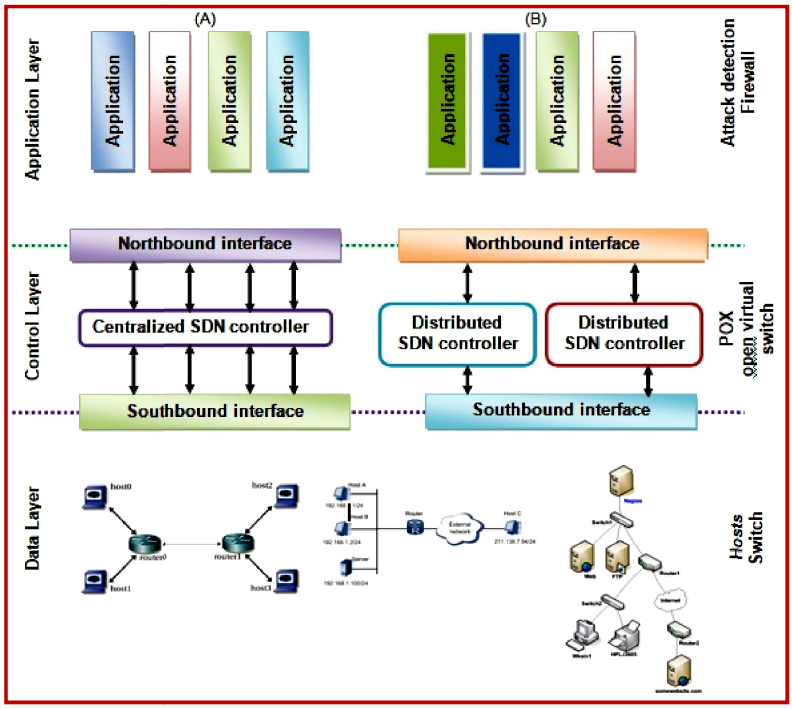

Figure 1. Basic SDN Architecture

The Internet of Things (IoT) has made it possible for basic electronic products to connect to a network. The expansion of the IoT has, however, raised significant security concerns. Implementing a robust security mechanism in an IoT context is a challenge, owing to the limited resources and battery life of the devices constituting the IoT network. The risks impacting IoT devices come in different forms and are growing. Attacks such as Distributed Denial-of-Service (DDoS) have become more prevalent with the development of the Internet of Things. IoT botnets can be employed, in addition to DDoS attacks, to disrupt the IoT network [4].

In recent years, however, the SDN-based IoT has provided a centralized or distributed controller with switches comprising different kinds of end nodes, including IoT end nodes. This work introduces the SDN controller with edge computing-enabled smart IoT devices in the forwarding layer, simultaneously using the middle layer framework while accessing cloud computing resources in the application layer. A new concept called "fog computing" pushes storage, communication, and compute capabilities out to the edge of networks. Fog computing uses little energy and suffers less traffic congestion than cloud computing, making it possible to serve time-sensitive end-user service requests.

Fog computing may be leveraged to improve cloud environments. Rather similar to a cloud environment, it is not as centralised. Fog computing has limited processing power, storage, and low data analytic capabilities. Further, it helps time-constrained real-time problems preserve their latency limitations, making them appropriate for use in Internet of Things (IoT)-based applications like smart health care monitoring and vehicular social networks [5].

Machine learning methods are used by the SDN controller to capture suspicious data flow and infer their validity. A distributed and localised processing strategy is used in fog computing-based DDoS mitigation. The three-level design of the fog computing-based DDoS mitigation method offers a comprehensive analysis of hostile network actions. Fog computing mitigates DDoS attacks efficiently because it coordinates and distributes computationally expensive tasks [6].

2. LITERATURE SURVEY

This section covers a basic survey of the literature and experimental work on SDN networks in relation to malicious DoS and DDoS attacks without the application of machine learning algorithms. A study by Azim et al. [7] suggested that routing issues be introduced in response to denial-of-service attacks. Accordingly, the proposed work creates a hybrid method to detect denial-of-service attacks and includes the data in routing decisions so as to identify and remove botnet nodes from the network at the earliest. For better outcomes, the proposed work intends to use and detect DDoS attacks in SDNs using ML algorithms.

A study by Kalliola et al. [8] described the plethora of attack modes that challenges the effective mitigation of distributed denial-of-service attacks. The proposed approach combines standard traffic learning with external blacklist data to deliver efficient load control, service flexibility, and filtering during attacks. The approach can sustain service quality for around 75% to 80% of regular clients.

Chin et al. discussed distributed network traffic monitors and correlators via the application of an OpenvSwitch (OvS) [9]. The paper also elaborates on the three fundamental SDN characteristics of scalability, flexibility, and monitoring that make SDNs indispensable. A method to stop TCP SYN flood attacks on the GENI testbed, barring a few restrictions, was suggested to help develop a DoS mitigation solution for SDNs.

Khan and Hameed [10] proposed a cooperative SDN-based DDoS attack mitigation technique. Developing a secure controller-to-controller protocol makes it possible for SDN controllers used in autonomous systems to communicate and share threat information with one another safely. We demonstrate that our SDN-based collaboration method is dependable and quick to prevent DDoS attacks efficiently in real time and with little processing.

3. RESEARCH PROBLEMS

Much of the earlier work on SDN environments concentrated on single or multi-centralized SDN controller architectures for DDoS attack detection with basic SDNs. The attack detection method employed in this instance is carried out using distributed SDN multicontroller architecture. The following issues have been identified in the current research:

- The average attack detection and classifier accuracy rates are to be improved.
- The execution time of the system is to be reduced.
- The number of attacks and types of attack detection are not up to the level, just as the precision, recall, and F1 score performance matrices are not up to the level and need improvement.

Furthermore, no study thus far has examined how well DDoS attack detection and mitigation performs when combined with IoT and fog layer processing on SDN distributed multicontrollers using machine learning techniques.

4. RESEARCH OBJECTIVES

This research presents a multi-faceted SDN-based solution in the event of a DDoS attack. DDoS attacks force SDN controllers to process malicious packets. The key contribution of the research, therefore, is to equip SDN controllers with DDoS detection mechanisms. The contributions of this research include the following:

- To demonstrate how a DDoS attack in distributed Multicontroller - SDN architecture can overload the controller
- To safeguard network application controller resources with an efficient DDoS detection methodology based on entropy and machine learning techniques

- To apply ML and SDN networking tools to implement the proposed mechanism and using numerous simulations to demonstrate the efficacy of the DDoS attack mitigation system

5. RESEARCH SOLUTIONS

5.1. The Detection and Mitigation of Distributed Denial-of-Service (DDOS) Attacks using the Entropy Method in Software-Defined Distributed Network Controllers

The proposed approach for entropy-based early attack detection is presented in this section. Software-defined networks are uniquely placed to separate the data plane and the control plane with their three layers (control, application, and infrastructure) and two interfaces (southbound and northbound). OpenFlow, an API developed for managing software- or hardware-based devices and controllers, is used here.

SDNs are unlikely to succeed in eradicating DDoS attacks entirely from networks. The proposed work explores SDN network security and creates a new methodology to detect DDoS attacks in a distributed multicontroller-based SDN environment, as shown in Figure 2.

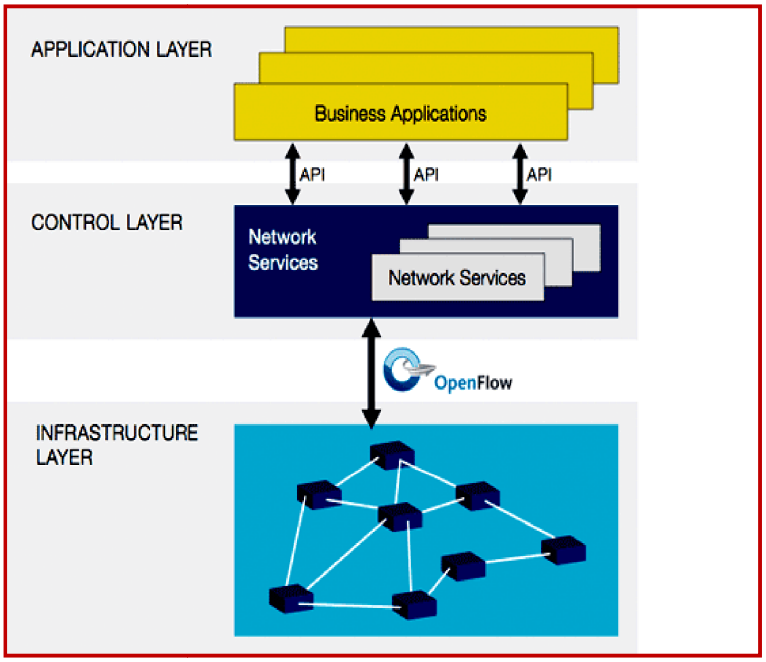

Figure 2. Software-Defined Networking Architecture

Proposed Methodology

This section explains the proposed DDOS attack detection and mitigation mechanism in a distributed multicontroller SDN environment, overcoming the shortcomings in the current centralised multicontroller design.

Based on the threshold level of the packets, the controllers determine whether malicious behaviour has been detected and decide which packets are to be forwarded or blocked. This analysis is updated in the controller database. Subsequently, other controllers in the distributed controller connection domain receive a message with the new analysis so that their databases can be updated. The OpenFlow switches and OpenFlow clients both send and receive all incoming packets.

Entropy-based DDoS detection requires a window size and a threshold. The entropy calculation of a window measures the degree of uncertainty in incoming packets. Depending on the system, an attack is anticipated if the estimated entropy exceeds or falls below a certain threshold. The packet is despatched to an output port if a rule is found. The parameters established in the controller will determine whether the controller forwards or blocks the packets.

Traffic Generation Module

Several programs may be employed for traffic generation. The packets, in this case, are created by the host level traffic.py Python program. Hosts 1, 2, and 3 provide regular traffic as a result of this module while the (attack.py) script produces the attack packet from the same host similarly. Both normal and attack traffic are generated between hosts 1 to 65 that are represented in the Mininet scenario. Based on the threshold and entropy conditions specified in the pox controller, the attack is recognized and action taken. Switches check incoming flow entries in accordance with the controller rule set.

Attack Detection Module

When a packet is blocked by the controller because of its high entropy value, a switch is activated to stop processing the client in question. The blocked information is sent to neighbouring controllers that are connected in the distributed environment for flow table updates to avoid repeating the mitigating operation in

every controller. The proposed work examines SDN network security based on a fusion of current techniques and creates a new DDoS attack detection method in a distributed controller-based SDN environment.

Experimental Setup

Table 1. Experimental setup for the SDN

S. No	Parameters	Description
1.	Emulator	Mininet
2.	Controller architecture	Distributed multicontroller
3.	Controller	POX
4.	Number of controllers	3
5.	Switch	Open Virtual Switch
6.	Interface	OpenFlow 1.3
7.	Number of clients	64
8.	Parameters	Traffic generation, attack generation and attack detection

Table 1 provides an overview of the parameters and experimental setup. Node 64 is considered the destination node and nodes 1, 2, and 3 the source nodes. Entropy, threshold value, and window size all play a part in the attack detection process while the amount of time or the number of packets determines window size. An attack is detected when the estimated entropy rises or lowers. Higher randomness equals higher entropy, and vice versa.

$$W = X1, X2, X3, \ldots\ldots \quad - \quad (3.1)$$

$$Pi = \frac{Xi}{n} \quad - \quad (3.2)$$

$$H = -\sum_{i=1}^{n} \quad Pi\ logPi \quad - \quad (3.3)$$

Pi is a statistical measure of how frequently an event occurs within a given window size.

RESULTS SUMMARY

Figure 3 displays an analysis of the DDOS attack detection and execution times, showing the sample packet counts used as a threshold value to calculate the attack and execution times for each packet count increase. Furthermore, it indicates that the controller can handle elevated attack packets quickly while raising the average execution time marginally.

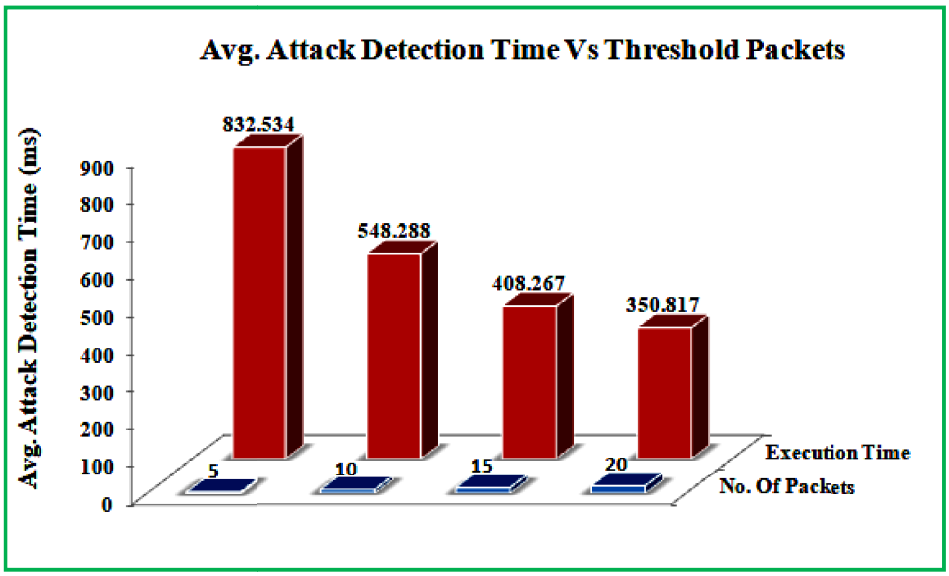

Figure 3. Average Attack Detection Time

5.2. Machine Learning-based Attack Detection and Mitigation in SDN-IOT Environments

DDoS attack mitigation directed towards Internet of Things nodes has, in recent years, garnered considerably more attention and produced more active research than traditional DDoS defence systems. Our study distributed multiple SDN controllers over the network and examined different end nodes using an IoT-based framework. The four modules that make up the proposed model include DDoS assault creation, attack mitigation, attack identification or detection, and recovery.

Software-defined networks are uniquely placed in that they separate the data plane and the control plane with their three layers (control, application, and infrastructure). The forwarding layer/data plane consists of SDN switches and IoT gateways. The middle layer's computing technology makes it easier to handle SDN controllers. The control layer or control plane is made up of several SDN controllers that are linked to a master SDN controller.

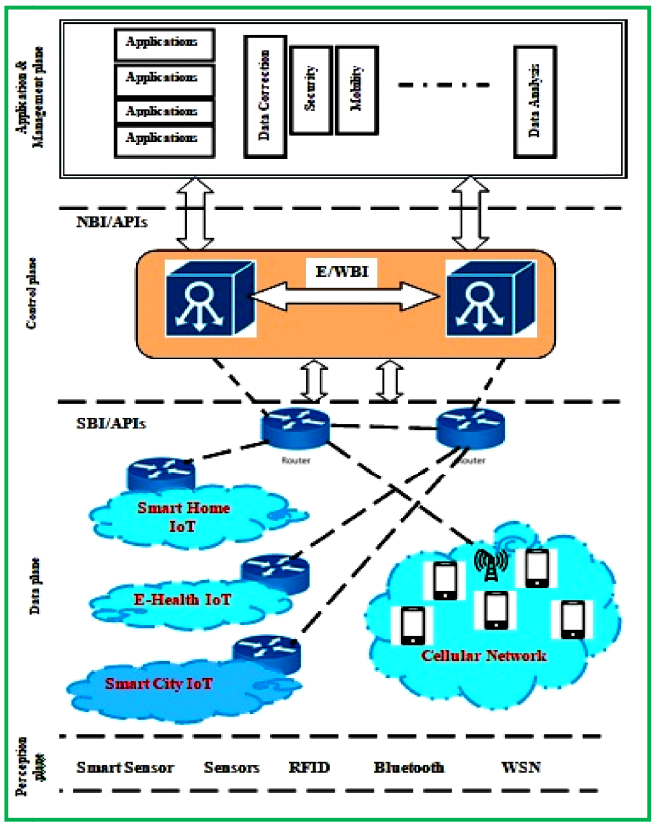

Figure 4. Proposed Model SDN-IoT Architecture

The proposed study has described the SDN-IoT-based machine learning-based DDoS attack mitigation process and assessed its effectiveness in comparison to the existing traditional DDoS attack detection method that does not use ML intelligence. Figure 4 displays the proposed IoT-SDN architecture.

In scenarios 1 and 2, which proposed an intelligent and free network paradigm and machine learning capabilities, a cluster of IoT and other computer devices was connected to a multi-layer multicontroller and SDN-based IoT switches in the network. The POX controller serves as a centralized/distributed SDN controller in single-controller or multicontroller configurations. Various machine learning classifiers were used to process and analyze the TCP, UDP, and ICMP packets from the entire dataset. This resulted in the transmission of benign data using 3,11,029 bandwidth packets, of which 1,54,401 were attack packets. In all, 30% was used for testing and 70% for training the entire benign dataset. The testing procedure revealed that the attack packets had successfully detected throughput of approx. 1,44,000.

EXPERIMENTAL ENVIRONMENT

A Python-based POX controller was utilized for the traditional SDN attack detection configuration in this experiment along with the virtual Oracle VMWare with the Mininet SDN setup. Our SDN testbed, shown in Table 2, was made up of hosts ranging from (1...100), switches from [1...9], and three controllers.

Table 2. Experimental Setup for the SDN-IOT

Components or Particulars	**Configuration Details**
System CPU and memory	Intel core i3-5005U @2.00Ghz / 4 GB, 64-bit OS
System operating system	Windows 10 Home Edition
Virtualization and guest OS	Oracle Virtual Box and Ubuntu 14.04
Other packages	Anaconda, Jupyter Notebook, Tensor Flow, Keras, Pandas, NumPy, Sklearn, Matplotlib and Pickle
Network emulation	Mininet 2.2.1
SDN controller type	Distributed
Forwarding element	Open v Switch
SDN controller	POX
Number of SDN controllers	09
Number of switches	09
Total number of clients/nodes	100

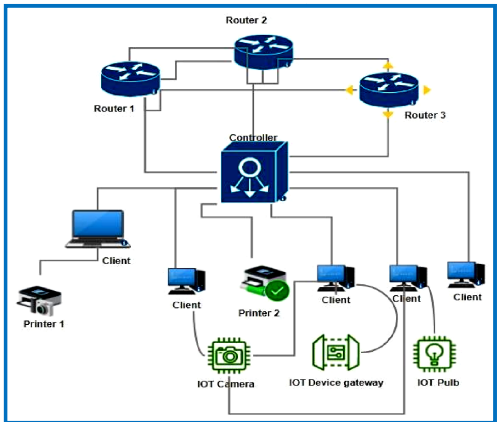

Figure 5. SDN Single-controller Architecture

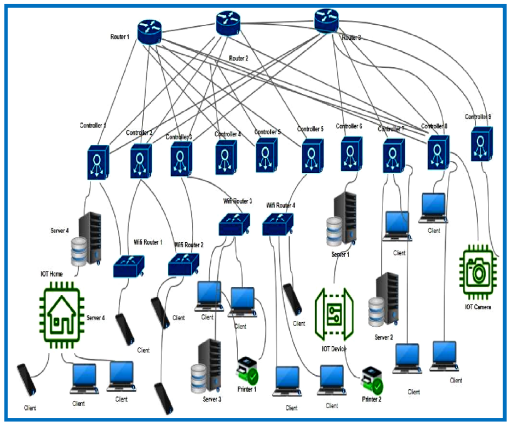

Figure 6. SDN Multicontroller Architecture

Much of our work has focused on detecting malicious DDoS behaviour in network data. Figures 5 and 6 illustrate how the experimental process first commenced with the use of a single-controller SDN network and a distributed multicontroller SDN without ML approaches.

RESULTS SUMMARY

The Anaconda tool and its framework were used for the experimental setup. Accuracy was computed for the trained datasets with ML-mitigated attacks using the true positive (TP), true negative (TN), false positive (FP), and false negative (FN) rates.

Table 3 presents the total of number of processed packet. It displays the number of regular and attack packets that the machine learning model was able to interpret by using additional packets from the raw datasets, together with the TCP, UDP, and ICMP protocol packets.

Table. 3. The number of Normal Vs Attack Packets

	ICMP	TCP	UDP	TOTAL
Number of Normal Packets	66145	74385	16098	156628
Number of Attack Packets	98824	44972	10605	154401
Total Packets	164969	119357	26703	311029

Figure 7 displays the average time, in milliseconds, needed to use ML algorithms and conventional approaches to resist a DDoS attack. The results show that it took 8.9 milliseconds for the standard attack detection algorithms of the distributed multicontroller network to identify and neutralize the attack. In contrast, the ML classification model finished the assignment in two to five milliseconds.

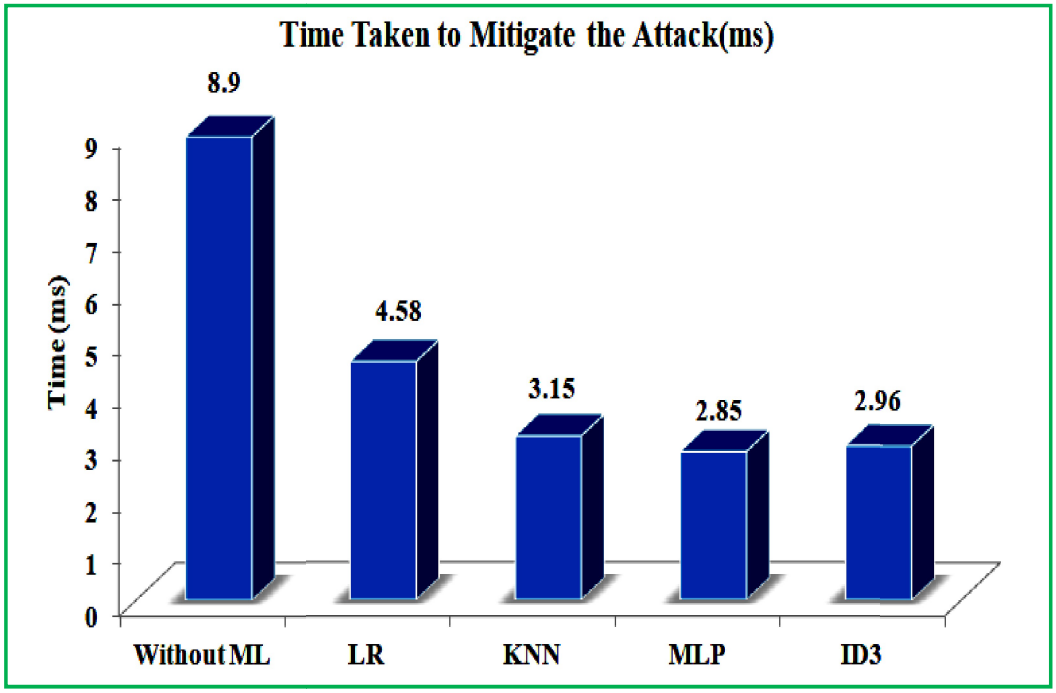

Figure 7. Time Taken to Mitigate Attacks with/without ML

5.3. MACHINE LEARNING-BASED DETECTION AND MITIGATION IN SDN-FOG ENVIRONMENTS

This study introduces the SDN controller in conjunction with edge computing smart Internet of Things devices in the forwarding layer, using the application layer cloud computing resource access framework and an intermediate fog computing layer framework.

Proposed Method

The objective of this study is to identify and neutralise attack traffic before it is sent to the resource server. To do this, a fog layer is constructed between the cloud resource server and the bottom layer. The fog layer is where malicious traffic is managed and dealt with. This study presents a framework for defending against DDoS attacks in an SDN-fog environment, as shown in Figure 8.

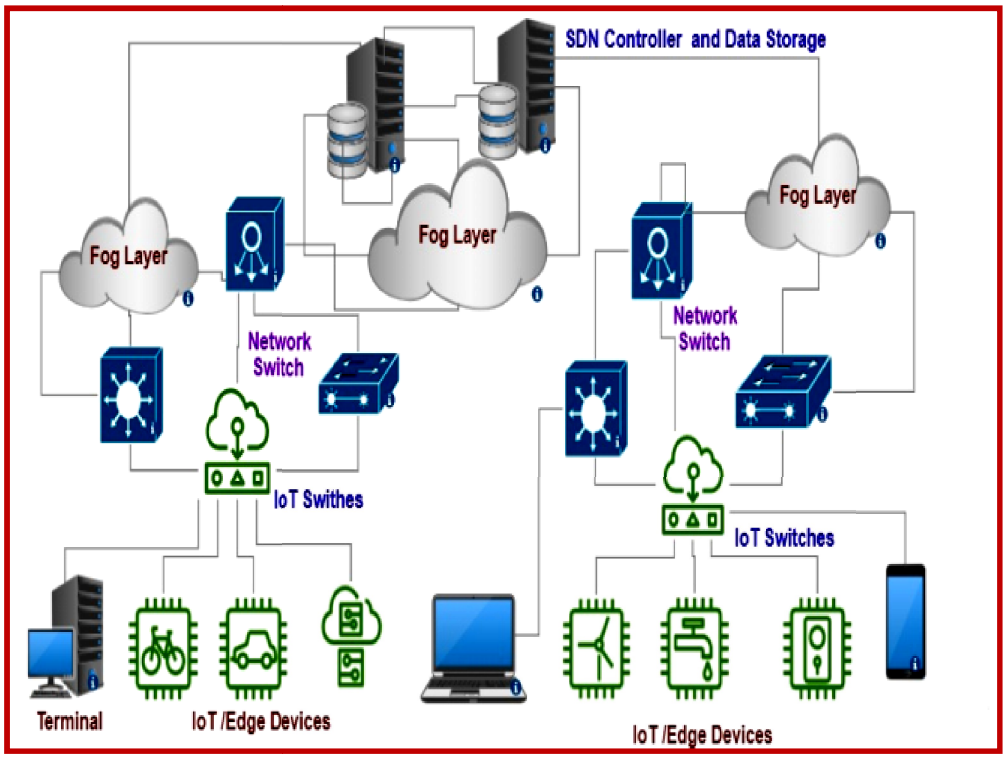

Figure 8. Proposed Model DDoS Attack Detection in the Fog-based SDN-IoT Network

SDN- FOG-IOT-based Network System

A machine learning technique is used to teach the SDN controller, also referred to as the fog server. The algorithms are trained using data from the incoming data flow, including Internet of Things devices. The target server receives the packet if it is deemed to be authentic. In case of a suspicious packet, the IP address of the relevant packet is added to the flow table of switches prohibited by the SDN controller. The target server cannot receive the packet because the switch level has completed the programming.

Experimental Results and Discussion

Data Sources

Tables 4 and 5 demonstrate the number of anomalous and regular packets from the raw IoT mixed dataset as well as the categories of attack traffic. The proposed study has employed the LR, KNN, MLP, and ID3 classifiers to detect and evaluate attacks in the distributed multicontroller SDN-fog-based IoT network.

Table 4. Attack and Normal Packet Sizes

S. No	Category	Packets
1.	Anomaly	137185
2.	Normal	112687
3.	Total	249872

Table 5. Dataset Description

S. No	Packet Type	Total Data Set Packets
1.	ICMP	65427
2.	TCP	48114
3.	UDP	23644
4.	Normal	112687
5.	Total	249872

The recall (R), F1-score (F1), accuracy (A), and precision performance metrics of machine learning models were used to calculate the performance of the attack detection process.

Results Summary

The SDN with IoT network datasets that included real-time DDoS attack packets constituted the experimental setup for ML attack detection and mitigation. Figure 9 depicts a model of the SDN-FOG-IOT network architecture which offers information on the clients connected to the fog switch, gateway, and SDN controller, as well as regular and malicious nodes. The quantum of network traffic data depends on the number of nodes. Assorted end nodes and physical layer nodes are found here. The IoT and SDN controllers are linked to the fog controller by switches in the fog layer, which is the middle layer. The higher layer contains the root SDN controller with established distributed connections among the controllers. Continuous packet transmission occurs between the switches and the fog controller as well as between attack nodes and ordinary end nodes.

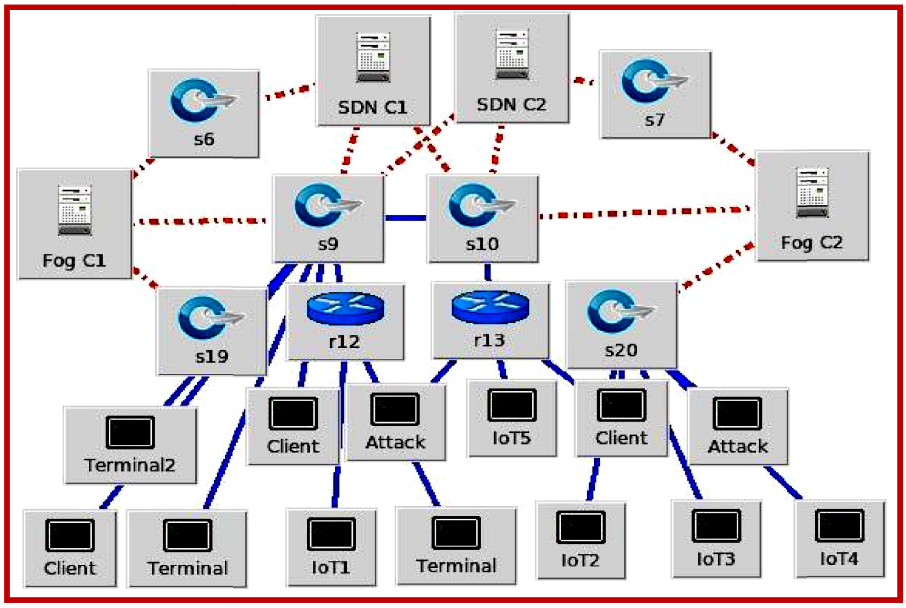

Figure 9. Model Experimental Setup of the Fog-based SDN-IoT Network

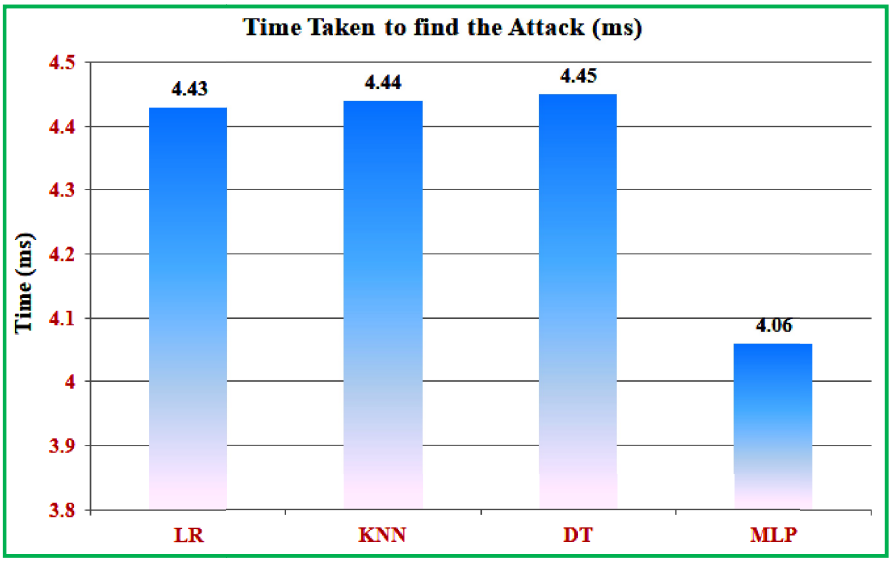

Figure 10. Time taken to find the attacks

Figure 10 displays the time taken to find the attacks using different classifiers. The aforementioned data suggest that the MLP Algorithm has taken the less time taken to identify the attack. In real custom dataset from IoT edge devices in a fog-based SDN multicontroller network environment, it was determined that the MLP algorithm takes 4.06 ms when compared to others.

6. THESIS ORGANIZATION

The thesis is organised in the manner described below:

- **Chapter 1,** Introduction, presents a background to software-defined networks and their elements, DDoS attacks, and attack detection and mitigation methods. Further, the impact of DDoS attacks and their effect on the controller are described.
- **Chapter 2,** Literature Review, discusses the literature on DDoS attack detection and mitigation in SDNs.
- **Chapter 3,** Entropy-based Detection and Mitigation using a Multicontroller. examines the proposed entropy-based approach to DDoS detection in the controller.
- **Chapter 4,** Machine Learning-based Attack Detection and Mitigation in SDN-IOT Environments, describes the experimental setup using the SDN-IoT and the outcomes of the experiment are analysed using machine learning.
- **Chapter 5,** Machine Learning-based Attack Detection and Mitigation in SDN-FOG Environments, describes the experimental setup using a fog-based SDN-IoT. The experimental data are analysed using machine learning.
- **Chapter 6,** Results and Discussion, presents the simulation results of the experimentation and discusses them. It concludes the thesis with a summary of the proposed approach.
- **Chapter 7,** Conclusions and Future Scope, dwells briefly on the limitations of the solution proposed and offers directions for future research.

7. CONCLUSIONS AND FUTURE SCOPE

This research has focused on detecting and mitigating DDoS attacks using a range of analytical techniques to deliver results in software-defined networking. It has implemented DDoS attack detection and mitigation strategies in a distributed multicontroller SDN system.

Firstly, unlike a centralized multicontroller network, the proposed technique leveraged distributed entropy-based DDoS attack detection and mitigation. To protect network controllers and link switches, it has demonstrated how to identify attack

packets from a specific group of source nodes and block them based on maliciously repeated packet IP addresses. However, in a limited situation, the proposed approach results in a limited attack detection output.

Secondly, this work was improved by providing the output and experimental results of an IoT-based SDN multicontroller network that uses machine learning methodologies. The results of traditional and machine learning-based DDoS attack detection systems have been investigated. DDoS attack detection accuracy using the LR, KNN, MLP, and RF machine learning methodologies was 93.4% surpassing that of conventional techniques. DDoS attack mitigation in the specialized SDN-IoT-based multicontroller model is more efficient than older approaches, as observed from a comparison of the present one.

As a result, the study included the fog intermediate layer in the SDN controller. This machine learning mechanism processed a customized dataset of around 2,50,000 packets, including 1,37,185 abnormal packets and 1,12,687 ordinary packets. A performance analysis yielded accuracy, precision, recall, and F1-score outcomes of 77%, 79%, 85%, and 81%, respectively. These findings suggest that the decision tree outperforms other classifiers in terms of performance.

Finally, this study was completed, based on the success of the three approaches above. For the SDN-IoT analysis, only the TCP, UDP, and ICMP protocols were employed, resulting in higher accuracy and performance in all other areas. However, when compared to the previous two approaches, the SDN-Fog-IoT-based machine learning method collected more attack packets from the total packets without a distinguishing packet classification process and produced better results.

However, in the future, the proposed method will be usefully enhanced with firewall protection and load balancing for a large number of controllers. Further, it will be expanded using current datasets with additional ML/DL algorithms in SDN multi-controller edge computing networks for DDoS attack mitigation, particularly in network applications featuring SDN controllers with failover mechanisms.

REFERENCES

1. Goyal P, Sahoo A K, Sharma T K, and Singh P K, Internet of Things: Applications, security and privacy: A survey, *Materials Today Proceedings,* **34** (3) (2021), 752-759.
2. Ezekiel S, Divakaran D M, and Gurusamy M, Dynamic attack mitigation using SDN, *2017 27th International Telecommunications Networks Applications. Conference*, (2017), 1–6.
3. Xu T, Gao D, Dong P, Zhang H, Foh C H, and Chao H C, Defending Against New-Flow Attack in SDN-Based Internet of Things, *IEEE Access*, **5**, (2017), 3431–3443.
4. Wani A and Revathi S, DDoS Detection and Alleviation in IoT using SDN, *Journal of the Institution of Engineers (India): Series B*, **101** (2020), 117-128.
5. Priyadarshini R, Kumar Barik R, and Dubey H, Fog-SDN: A light mitigation scheme for DDoS attack in a fog computing framework, *International Journal of Communication Systems,* **33**(9) (2020), 1–13.
6. Zhou L, Guo H, and Deng G, A fog computing-based approach to DDoS mitigation in IIoT systems, *Computer Security*, **85** (2019), 51–62.
7. Abdel Azim N M, Fahmy S F, Sobh M A, and Bahaa Eldin A M, A hybrid entropy-based DoS attacks detection system for software defined networks (SDN): A proposed trust mechanism, *Egyptian Informatics Journal,* **22**(1) (2021), 85-90.
8. Kalliola A, Lee K, Lee H, and Aura T, Flooding DDoS mitigation and traffic management with software defined networking, *2015 IEEE International Conference on Cloud Networking,* (2015), 248–254.
9. Chin T, Mountrouidou X, Li X and Xiong K, An SDN-supported collaborative approach for DDoS flooding detection and containment, *MILCOM, 2015 IEEE Military Communications Conference*, Tampa, FL, USA, (2015), 659-664.
10. Hameed S and Khan H A, SDN-based collaborative scheme for mitigation of DDoS attacks, *Future Internet*, **10** (3) (2018), 23.

List of Publications

1. Kavitha D, Ramalakshmi R, Machine Learning-based DDOS Attack Detection and Mitigation in SDNs for IoT Environments, *Journal of the Franklin Institute.* **361**(17) (2024).
2. Kavitha D, Ramalakshmi R, DDoS Attack Mitigation using Distributed SDN Multicontrollers for Fog-based IoT Systems, *International Journal of Intelligent Systems and Applications in Engineering*, **12**(4s), (2024) 57–69.
3. Kavitha D, Ramalakshmi R, Fog-based SDN for DDOS Attack Mitigation in IoT Systems: A Survey, *International Journal of Future Generation Communication and Networking*, **13**(4) (2020), 4161–4173.
4. Kavitha D, Ramalakshmi R and Murugeswari R, The Detection and Mitigation of Distributed Denial-of-Service (DDOS) Attacks in Software Defined Networks using Distributed Controllers, *2019 IEEE International Conference on Clean Energy and Energy-Efficient Electronics Circuit for Sustainable Development (INCCES)*, Krishnankoil, India, (2019), 1-5.